6712-01

This document is scheduled to be published in the Federal Register on 09/08/2021 and available online at **federalregister.gov/d/2021-18683**, and on **govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

[FR ID: 45237]

Privacy Act of 1974; System of Records.

AGENCY: Federal Communications Commission

ACTION: Notice of a modified system of records.

SUMMARY: The Federal Communications Commission (FCC or Commission or Agency) has modified an existing system of records, FCC/OMD-16, Personnel Security Files, subject to the Privacy Act of 1974, as amended. This action is necessary to meet the requirement of the Privacy Act to publish in the Federal Register notice of the existence and charger of records maintained by the agency. The FCC's Security Operations Center (SOC) in the Office of Managing Director (OMD) uses this system of records to determine an individual's suitability for access to classified information and/or a security clearance; evaluate an individual's suitability for Federal employment, including temporary hires such as interns, consultants, and experts, or to perform contractual services for the FCC; respond to complaints of threats, harassment, violence, or other inappropriate behavior at the FCC; and, document security violations and related activities such as insider threats.

DATES: This system of records will become effective on **[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Written comments on the routine uses are due by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. The routine uses will become effective on [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**], unless written comments are received that require a contrary determination.

ADDRESSES: Send comments to Margaret Drake, at privacy@fcc.gov, or at Federal Communications Commission, 45 L Street, NE, Washington, DC 20554 at (202) 418-1707.

FOR FURTHER INFORMATION CONTACT: Margaret Drake, (202) 418-1707, or privacy@fcc.gov (and to obtain a copy of the Narrative Statement and the Supplementary Document, which includes details of the modifications to this system of records).

SUPPLEMENTARY INFORMATION: This notice serves to modify FCC/OMD-16, Personnel Security Files, to reflect various necessary updates, including format changes required by OMB Circular A-108 since its previous publication and edits to existing routine uses, two of which address data breaches, as required by OMB Memorandum M-17-12. The substantive changes and modifications to the previously published version of the FCC/OMD-16 system of records include:

1. Updating the System Location to show the FCC's new headquarters address.
2. Updating the Purposes section for clarity and to include determinations about an individual's suitability, eligibility, and fitness to access FCC and other Federal facilities, information, systems, or applications.
3. Updating the Categories of Individuals Covered section for clarity and to include witnesses, references, and other individuals who may have provided information contained in this system.
4. Updating the Categories of Records for clarity and to include information related to maintenance of a public trust or national security position.
5. Renumbering and revising language in four routine uses: (2) Law Enforcement and Investigation; (4) Government-wide Program Management and Oversight; (9) Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by Other than the FCC, and (10) Labor Relations.
6. Removing two routine uses: (5) Contract Services, Grants, or Cooperative Agreements and (13) National Security and Intelligence Matters.
7. Adding a new Routine Use: (14) For Non-Federal Personnel, to allow contractors performing or working on a contract for the Federal Government access to information in this system.
8. Updating the History section referencing the previous publication of this SORN in the Federal Register, as required by OMB Circular A-108.

The system of records is also updated to reflect various administrative changes related to the system managers and system addresses; policy and practices for storage, retrieval, and retention and disposal of the records; administrative, technical, and physical safeguards; and updated notification, records

access, and contesting records procedures.

SYSTEM NAME AND NUMBER:

FCC/OMD-16, Personnel Security Files.

SECURITY CLASSIFICATION:

Most personnel identity verification records are not classified. However, in some cases, records of certain individuals, or portions of some records may have national defense/foreign policy classifications.

SYSTEM LOCATION:

Security Operations Center, Office of Managing Director (OMD), Federal Communications Commission (FCC), 45 L Street, NE, Washington, DC, 20554.

SYSTEM MANAGER(S):

Security Operations Center (SOC), Office of the Managing Director (OMD), Federal Communications Commission, (FCC), 45 L Street, NE, Washington, DC, 20554.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 1303, 1304, 3301, 7902, 9101; 42 U.S.C. 2165 and 2201; 50 U.S.C. 781 to 887; 5 CFR Parts 5, 732, and 736; Executive Orders 9397, 10450, 10865, 12196, 12333, 12356, and 12674, 13587; and Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

PURPOSE(S) OF THE SYSTEM:

The FCC must document, support, and track its decisions regarding personnel security. The SOC uses the information in this system to document and track:

1. Determinations about an individual's suitability, eligibility, and fitness for Federal employment, as well as access to classified information or restricted areas and security clearances;
2. Determinations about an individual’s suitability, eligibility, and fitness to perform contractual services for the U.S. Government;

3. Determinations about an individual's suitability, eligibility, and fitness to access FCC and other Federal facilities, information, systems, or applications, and documenting such determinations;
4. Investigate, respond, document, and track complaints about inappropriate workplace behavior; and
5. Document security violations, such as insider threats, and management actions taken in response to those violations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The individuals in this system include:

1. Current and former FCC employees, including full and part time employees, interns, detailees, and volunteers;
2. Current and former contractor employees and prospective contractor employees, for whom an investigation is initiated and/or conducted;
3. Individuals who are authorized to perform, provide, or to use services in FCC facilities (either on an ongoing or occasional basis), such as security personnel, custodial staff, maintenance workers, contractors, health clinic staff, and employee assistance program staff;
4. All other individuals who may require regular on-going access to the FCC's buildings and facilities, information technology (IT) systems, or information classified in the interest of national security, as well as individuals formerly in any of these positions;
5. Witnesses, references, and other individuals who have provided information about the subject of an investigation documented in this system;
6. Individuals who may be involved with potential, alleged, or actual security violations, including insider threat activity.

CATEGORIES OF RECORDS IN THE SYSTEM: The categories of records include:

1. Personally identifiable information from Standard Form 85 " Questionnaire for Non-Sensitive Positions," Standard Form 85P "Questionnaire for Public Trust Positions," Standard Form 85P-S "Supplemental Questionnaire for Selected Positions," Standard form 86 "Questionnaire for National Security Position," and predecessor and successor forms of the

same type; copies of investigative reports from other federal agencies; correspondence, information, and other supporting documentation related to the investigation, adjudication, and maintenance of public trust and national security information positions;

2. Information needed to investigate allegations of misconduct, including insider threats and complaints not covered by the FCC's formal or informal grievance procedures.

RECORD SOURCE CATEGORIES:

Under the authority granted to heads of agencies by 5 U.S.C. 552a (k), the FCC has determined (47 CFR Section 0.561) that this system of records is exempt from disclosing its record sources for this system of records.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside the FCC as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows.

1. Adjudication and Litigation – To disclose information to the Department of Justice (DOJ), or other administrative body before which the FCC is authorized to appear, when: (a) the FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where DOJ or the FCC has agreed to represent the employee; or (d) the United States is a party to litigation or has an interest in such litigation, and the use of such records by DOJ or the FCC is deemed by the FCC to be relevant and necessary to the litigation.
2. Law Enforcement and Investigation – To disclose pertinent information to the appropriate Federal, State, local, or tribal agency, or component of an agency, such as the FCC’s Enforcement Bureau, responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the FCC becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.
3. Congressional Inquiries – To provide information to a Congressional office from the record

of an individual in response to an inquiry from that Congressional office made at the request of that individual.

4. Government-wide Program Management and Oversight – To disclose information to the Department of Justice (DOJ) to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); to the Office of Management and Budget (OMB) to obtain that office's advice regarding obligations under the Privacy Act.
5. Non-FCC Individuals and Organizations – To individuals, including former FCC employees, and organizations in the course of an investigation to the extent necessary to obtain information pertinent to the investigation.
6. Complainants and Victims – To individual complainants and/or victims to the extent necessary to provide such individuals with information and explanations concerning the progress and/or results of the investigation or case arising from the matter of which they complained and/or of which they were a victim.
7. Office of Personnel Management (OPM) – To OPM management, Merit Systems Protection Board, Equal Opportunity Employment Commission, Federal Labor Relations Authority, and the Office of Special Counsel for the purpose of properly administering Federal personnel systems or other agencies' systems in accordance with applicable laws, Executive Orders, and regulations.
8. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the FCC – To a Federal, State, local, foreign, tribal, or other public agency or authority maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the hiring or retention of an employee or other personnel action, the issuance or retention of a security clearance, the classifying of jobs, the letting of a contract, or the issuance or retention of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decisions on the matter.
9. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by Other

than the FCC – To a Federal, State, local, foreign, tribal, or other public agency or authority of the fact that this system of records contains information relevant to the hiring or retention of an employee, the issuance or retention of a security clearance, the conducting of a suitability or security investigation of an individual, the classifying of jobs, the letting of a contract, or the issuance or retention of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the agency's decision on the matter.

10. Labor Relations – To officials of labor organizations recognized under 5 U.S.C. Chapter 71 consistent with provisions in an effective collective bargaining agreement or upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.
11. Security Officials and Investigators – To Security Officials and investigators of Federal Government agencies or departments for liaison purposes where appropriate during meetings or conferences involving access to classified materials.
12. Breach Notification – To appropriate agencies, entities, and person when (1) the Commission suspects or has confirmed that there has been a breach of the system of records; (2) the Commission has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Commission (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with Commission efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
13. Assistance to Federal Agencies and Entities – To another Federal agency or Federal entity, when the Commission determines that information from this system is reasonably necessary to assist the recipient agency or entity in: (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, program, and operations), the Federal

Government, or national security, resulting from a suspected or confirmed breach.

14. For Non-Federal Personnel – To disclose information to non-Federal personnel, i.e., contractors, performing or working on a contract in connection with the Security Operations Center and/or IT services for the Federal Government, who may require access to this system of records.

REPORTING TO A CONSUMER REPORTING AGENCIES:

In addition to the routine uses cited above, the Commission may share information from this system of records with a consumer reporting agency regarding an individual who has not paid a valid and overdue debt owed to the Commission, following the procedures set out in the Debt Collection Act, 31 U.S.C. 3711(e).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Electronic data, records, and files are maintained in a stand-alone computer database hosted on FCC's computer network.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by an individual's name or Social Security Number (SSN).

POLICIES AND PRACTIES FOR RETENTION AND DISPOSAL OF RECORDS:

The records in this information system are retained and disposed of in accordance with General Records Schedule (GRS) 5.6, items 180 and 181 (also referred to as DAA-GRS-2017-006-0024 / 0025), approved by the National Archives and Records Administration (NARA).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The electronic records, data, and files are stored within FCC accreditation boundaries and maintained in a database housed in the FCC computer network. Access to the electronic files is restricted to authorized SOC staff and contractors, and IT staff, contractors, and vendors who maintain the IT networks and services. As a further measure, access to these electronic records is restricted to the SOC staff and contractors who have a specific role in the system that requires their access to investigation information and related SOC functions. The SOC maintains an audit trail to monitor access. Furthermore, as part of these privacy and security requirements, SOC staff and contractors must complete training specific to their roles to ensure that they are

knowledgeable about how to protect PII. Other FCC employees and contractors may be granted access on a need-to-know basis. The electronic files and records are protected by the FCC and third-party privacy safeguards, a comprehensive and dynamic set of IT safety and security protocols and features that are designed to meet all Federal IT privacy standards, including those required by the Federal Information Security Modernization Act of 2014 (FISMA), the Office of Management and Budget (OMB), and National Institute of Standard and Technology (NIST).

RECORD ACCESS PROCEDURES:

Under the authority granted to heads of agencies by 5 U.S.C. 552a (k), the FCC has determined (47 CFR Section 0.561) that this system of records is exempt from disclosing its record access procedures for this system of records.

CONTESTING RECORD PROCEDURES:

Individuals wishing to request access to and/or amendment of records about themselves should follow the Notification Procedure below.

NOTIFICATION PROCEDURES:

Individuals wishing to determine whether this system of records contains information about themselves may do so by writing Privacy@fcc.gov. Individuals requesting access must also comply with the FCC's Privacy Act regulations regarding verification of identity to gain access to records as required under 47 CFR part 0, subpart E.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

This system of records is exempt from sections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f) of the Privacy Act of 1974, 5 U.S.C. 552a, and from 47 CFR Sections 0.554 – 0.557 of the Commission's rules. These provisions concern the notification, record access, and contesting procedures described above, and also the publication of record sources. The system is exempt from these provisions because it contains the following types of information:

1. Properly classified information, obtained from another Federal agency during the course of a personnel investigation, which pertains to national defense and foreign policy, as stated in Section (k)(1) of the Privacy Act;

2. Investigative material compiled for law enforcement purposes as defined in Section (k)(2) of the Privacy Act;
3. Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, as described in Section (k)(5) of the Privacy Act, as amended.

HISTORY:

The FCC last gave full notice of this system of records, FCC/OMD-16, Personnel Security Files, by publication in the Federal Register on March 12, 2018 (83 FR 10721).

Federal Communications Commission.

Marlene Dortch,

Secretary.

[FR Doc. 2021-18683 Filed: 9/7/2021 8:45 am; Publication Date: 9/8/2021]